BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

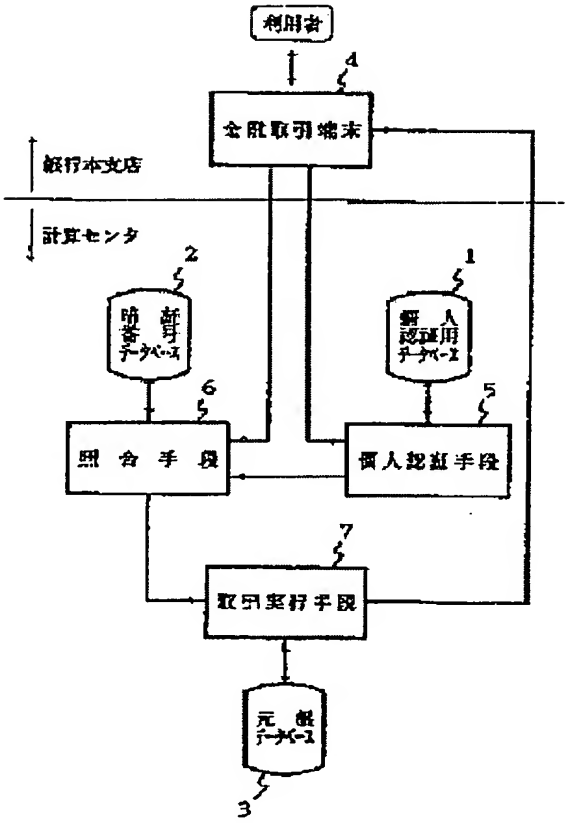
FINANCIAL TRANSACTION SYSTEM UTILIZING INDIVIDUAL AUTHENTICATION

Patent number:	JP11338947
Publication date:	1999-12-10
Inventor:	NOZATO KATSUJI
Applicant:	OKINAWA NIPPON DENKI SOFTWARE KK
Classification:	
- international:	G06F19/00; G06T7/00
- european:	
Application number:	JP19980144217 19980526
Priority number(s):	

Abstract of **JP11338947**

PROBLEM TO BE SOLVED: To provide a service capable of a transaction as long as a user is the person himself or herself even when the user forgets the password number does not or carry a bankbook and a card by adding individual confirmation by the individual authentication information such as a fingerprint or the like to a present system.

SOLUTION: A user who registers the individual authentication information of the fingerprint or the like can perform the transaction by a financial transaction terminal 4 provided with a fingerprint sampling function even in the case of forgetting the identification number and the case of not carrying the bankbook and the card. A calculation center is provided with a data base 1 for individual authentication storing name, individual authentication information, account number and identification number and individual authentication means 5 in addition to a pass password number data base 2, a ledger data base 3, a collation means 6 and a transaction execution means 7. In the case of the transaction without the bankbook and the card, the inputted name and a sample fingerprint feature are transferred to the individual authentication means 5 and collated with the individual authentication information retrieved by the name, and when they match with each other, the pertinent account number and password number are sent to the collation means 6, and thereafter, the password number is collated and the transaction is performed by a normal procedure. In the case of forgetting the password number, the bankbook and the card are inserted, the fingerprint is inputted and the transaction is performed.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－338947

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ	15/30	３４０
Ｇ０６Ｔ　7/00			15/62	４６０

審査請求　有　　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平10－144217

(22)出願日　平成10年(1998)５月26日

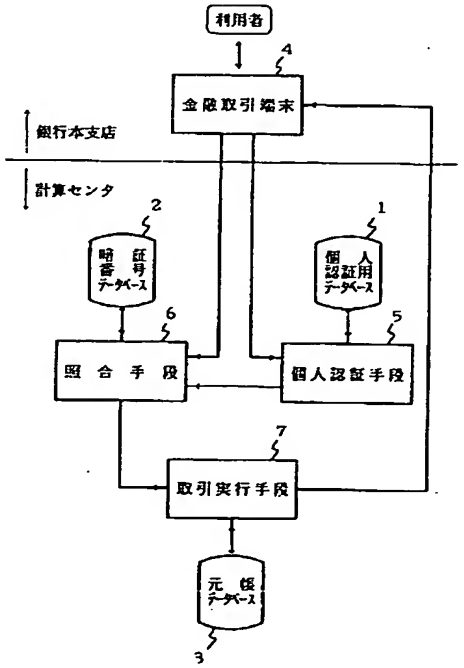
(71)出願人　000123262
沖縄日本電気ソフトウェア株式会社
沖縄県那覇市久米２丁目３番15号

(72)発明者　野里　勝治
沖縄県那覇市久米２丁目３番15号　沖縄日本電気ソフトウェア株式会社内

(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　個人認証を利用した金融取引方式

(57)【要約】
【課題】指紋等の個人認証情報による本人確認を現行方式に付加し、本人なら暗証番号を忘れたり通帳やカードを携帯せずとも取引可能なサービスを提供する。
【解決手段】指紋等の個人認証情報を登録した利用者は、指紋採取機能を備えた金融取引端末４で、暗証番号を忘れた場合や通帳，カードを携帯しない場合も取引できる。計算センタには、通常の暗証番号データベース２，元帳データベース３，照合手段６，取引実行手段７に加え、氏名，個人認証情報，口座番号，暗証番号を格納した個人認証用データベース１と個人認証手段５がある。通帳，カードなしの取引の場合、入力した氏名と採取した指紋特徴が個人認証手段５に転送され、氏名で検索した個人認証情報と照合し、一致すれば該当する口座番号と暗証番号が照合手段６に送られ、以降通常の手順で暗証番号を照合し取引が行われる。暗証番号を忘れた場合、通帳，カードを挿入し指紋を入力して取引を行う。



1

【特許請求の範囲】

【請求項１】　氏名を主検索キーとして本人確認用の個人認証情報と口座番号と暗証番号とを格納した個人認証用データベースと、口座番号と暗証番号とを対応させて格納した暗証番号データベースと、口座番号ごとの金融取引情報が格納されている元帳データベースと、個人認証情報を採取し前記個人認証用データベースと照合するために転送する機能を備えた金融取引端末と、前記金融取引端末から転送された氏名または口座番号と個人認証情報とで前記個人認証用データベースを参照して本人であることを確認し口座番号と暗証番号との両者または暗証番号のみを出力する個人認証手段と、前記金融取引端末または個人認証手段からの口座番号および暗証番号を前記暗証番号データベースと照合して確認する照合手段と、前記照合手段により確認されたとき前記金融取引端末からの取引要求を前記元帳データベースを参照して実行する取引実行手段とを備えていることを特徴とする個人認証を利用した金融取引方式。

【請求項２】　前記個人認証用データベース及び個人認証手段が複数の金融機関に共通に設けられ、前記個人認証用データベースには副検索キーとして金融機関識別情報が格納されていることを特徴とする請求項１記載の個人認証を利用した金融取引方式。

【請求項３】　前記個人認証用データベース及び個人認証手段が本人確認を業務とする個人認証機関に設けられ、前記個人認証用データベースと照合するための情報は前記金融取引端末からオープンネットワークを介して前記個人認証機関に転送され、前記個人認証手段からの口座番号および暗証番号は専用線を使用して前記照合手段に転送されることを特徴とする請求項１記載の個人認証を利用した金融取引方式。

【請求項４】　口座番号を主検索キーとして本人確認用の個人認証情報と暗証番号とを格納した個人認証用データベースと、口座番号と暗証番号とを対応させて格納した暗証番号データベースと、口座番号ごとの金融取引情報が格納されている元帳データベースと、個人認証情報を採取し前記個人認証用データベースと照合するために転送する機能を備えた金融取引端末と、前記金融取引端末から転送された口座番号と個人認証情報とで前記個人認証用データベースを参照して本人であることを確認し暗証番号を出力する個人認証手段と、前記金融取引端末または個人認証手段からの口座番号および暗証番号を前記暗証番号データベースと照合して確認する照合手段と、前記照合手段により確認されたとき前記金融取引端末からの取引要求を前記元帳データベースを参照して実行する取引実行手段とを備えていることを特徴とする個人認証を利用した金融取引方式。

【請求項５】　前記口座番号が金融機関の識別情報を含み、前記個人認証用データベース及び個人認証手段が複数の金融機関に共通に設けられていることを特徴とする請求項４記載の個人認証を利用した金融取引方式。

【請求項６】　前記個人認証情報が指紋情報であることを特徴とする請求項１，請求項２，請求項３，請求項４又は請求項５のいずれかに記載の個人認証を利用した金融取引方式。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は個人認証を利用した金融取引方式に関し、特に暗証番号を忘れた場合や、通帳もキャッシュカードも携帯していない場合でも、本人であれば複雑な手続きをせず現金払い出しが行える個人認証を利用した金融取引方式に関する。

【０００２】

【従来の技術】現在、銀行等の金融機関における預貯金の払い出しは、通帳またはキャッシュカードと暗証番号とを併用して行う金融取引端末（現金自動入出金機：ＡＴＭ）による自動取引が主体となっている。この現行方式は、利用者は暗証番号さえ覚えておけば、通帳がなくても携帯容易なキャッシュカードを使用して自分の口座から必要な現金の払い出しを行うことができ、使いやすく便利な方式である。更に、通帳やキャッシュカードを紛失し他人に拾得された場合でも、暗証番号が一致しなければ払い出しができないため、安全性の面でも必要な配慮がなされていると言える。

【０００３】上述の現行方式に対する改善策として、入力時のキー操作から暗証番号が判読されるのを防止する方法や、キャッシュカードに指紋情報を磁気データとして登録しておき、カードの使用者が本人であることを確認して取引を行う方式（実用新案：第３０４３０６１号）や、カードを使用せず指紋と暗証番号とを併用して本人識別を行う方式（実開平１－１２７０５１号）など、安全性を更に向上させるための幾つかの提案が見られる。しかしながら、これらのうち指紋を使用する方法は、本人以外の取引を認めないことになるため、悪意のない親族などの代理行為をも不可能とするものであり、全面的な採用は現実的には困難である。

【０００４】一方、現行方式の問題点として、本人であっても暗証番号を忘れた場合には取引ができず、登録した暗証番号を問い合わせるためには本人確認を含む面倒な手続が必要となること、通帳もキャッシュカードも携帯していない場合には、本人であっても取引ができないことなどが挙げられる。しかしながら、これらの問題点を解決するための提案はほとんど見受けられない。

【０００５】

【発明が解決しようとする課題】上述したように、通帳またはキャッシュカードと暗証番号とを併用する現行の金融取引方式は、利用者にとって便利であり安全性も確保されているが、本人でも暗証番号を忘れた場合や、通帳もキャッシュカードも携帯していない場合には取引ができないという改善すべき課題が残されている。

3

【０００６】これらを解決するために、本人確認に指紋を利用することが考えられるが、前述したキャッシュカードに指紋情報を登録する実用新案：第３０４３０６１号の方法では、キャッシュカードを携帯していない場合に対応できず、指紋と暗証番号とを併用する実開平１－１２７０５１号の方法では、暗証番号を忘れた場合には対応できない。

【０００７】本発明の目的は、個人特有の指紋等の個人認証情報を利用した本人確認を現行方式に併用することにより、本人であれば暗証番号を忘れた場合や通帳もキャッシュカードも携帯していない場合でも取引を可能とするなど、サービスの向上が可能となる個人認証を利用した金融取引方式を提供することである。

【０００８】

【課題を解決するための手段】請求項１の個人認証を利用した金融取引方式は、氏名を主検索キーとして本人確認用の個人認証情報と口座番号と暗証番号とを格納した個人認証用データベースと、口座番号と暗証番号とを対応させて格納した暗証番号データベースと、口座番号ごとの金融取引情報が格納されている元帳データベースと、個人認証情報を採取し前記個人認証用データベースと照合するために転送する機能を備えた金融取引端末と、前記金融取引端末から転送された氏名または口座番号と個人認証情報とで前記個人認証用データベースを参照して本人であることを確認し口座番号と暗証番号との両者または暗証番号のみを出力する個人認証手段と、前記金融取引端末または個人認証手段からの口座番号および暗証番号を前記暗証番号データベースと照合して確認する照合手段と、前記照合手段により確認されたとき前記金融取引端末からの取引要求を前記元帳データベースを参照して実行する取引実行手段とを備えて構成されている。

【０００９】請求項２の個人認証を利用した金融取引方式は、請求項１記載の個人認証を利用した金融取引方式において、前記個人認証用データベース及び個人認証手段が複数の金融機関に共通に設けられ、前記個人認証用データベースには副検索キーとして金融機関識別情報が格納されていることを特徴としている。

【００１０】請求項３の個人認証を利用した金融取引方式は、請求項１記載の個人認証を利用した金融取引方式において、前記個人認証用データベース及び個人認証手段が本人確認を業務とする個人認証機関に設けられ、前記個人認証用データベースと照合するための情報は前記金融取引端末からオープンネットワークを介して前記個人認証機関に転送され、前記個人認証手段からの口座番号および暗証番号は専用線を使用して前記照合手段に転送されることを特徴としている。

【００１１】請求項４の個人認証を利用した金融取引方式は、口座番号を主検索キーとして本人確認用の個人認証情報と暗証番号とを格納した個人認証用データベースと、口座番号と暗証番号とを対応させて格納した暗証番号データベースと、口座番号ごとの金融取引情報が格納されている元帳データベースと、個人認証情報を採取し前記個人認証用データベースと照合するために転送する機能を備えた金融取引端末と、前記金融取引端末から転送された口座番号と個人認証情報とで前記個人認証用データベースを参照して本人であることを確認し暗証番号を出力する個人認証手段と、前記金融取引端末または個人認証手段からの口座番号および暗証番号を前記暗証番号データベースと照合して確認する照合手段と、前記照合手段により確認されたとき前記金融取引端末からの取引要求を前記元帳データベースを参照して実行する取引実行手段とを備えて構成されている。

【００１２】請求項５の個人認証を利用した金融取引方式は、請求項４記載の個人認証を利用した金融取引方式において、前記口座番号が金融機関の識別情報を含み、前記個人認証用データベース及び個人認証手段が複数の金融機関に共通に設けられていることを特徴としている。

【００１３】請求項６の個人認証を利用した金融取引方式は、請求項１，請求項２，請求項３，請求項４又は請求項５のいずれかに記載の個人認証を利用した金融取引方式において、前記個人認証情報が指紋情報であることを特徴としている。

【００１４】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００１５】図１は、本発明の第１の実施の形態の構成を示すブロック図である。図１に示す本実施の形態は、本発明の個人認証を利用した金融取引方式の基本的な構成であり、指紋等の個人認証情報が格納されている個人認証用データベース１と、口座番号と暗証番号とが対比して格納されている暗証番号データベース２と、口座番号ごとの金融取引情報が格納されている元帳データベース３と、指紋等の個人認証情報を採取し転送する機能を備えた金融取引端末４と、金融取引端末４からの個人認証情報と氏名または口座番号とにより個人認証用データベース１を参照して本人確認を行い口座番号と暗証番号との両者または暗証番号のみを出力する個人認証手段５と、金融取引端末４または個人認証手段５から受け取った口座番号と暗証番号を暗証番号データベース３と照合して確認する照合手段６と、照合手段６により確認されたとき金融取引端末４からの取引要求を元帳データベース３を参照して実行する取引実行手段７とを備えて構成されている。

【００１６】上述の各構成要素のうち、個人認証用データベース１，暗証番号データベース２，元帳データベース３，個人認証手段５，照合手段６及び取引実行手段７は、銀行等の金融機関の計算センタに設置されており、本店および各支店に設置され利用者が操作する金融取引

端末４とは、専用線により接続されている。金融取引端末４は、あらかじめ指紋等の個人認証情報を登録した利用者が、暗証番号を忘れた場合や通帳もキャッシュカードも携帯していない場合にも取引できる端末であり、通常の現金自動入出金機の機能に加えて、指紋を採取する指紋採取部と採取した指紋イメージを解析し指紋特徴を抽出する特徴解析部とを備えている。なお、図１には示してないが、銀行本支店には、現行の通帳，キャッシュカードと暗証番号とを使用する通常の現金自動入出金機も設置され併用される。

【００１７】個人認証用データベース１は、あらかじめ登録した利用者の個人認証情報が格納されているデータベースであり、氏名を主検索キーとして個人認証情報，口座番号，暗証番号が格納されており、口座番号を検索キーとする検索も行えるようになっている。

【００１８】次に、図１の動作について説明する。まず、通帳，キャッシュカードと暗証番号とを使用する通常の金融取引の場合には、利用者が挿入した通帳またはキャッシュカードに記録されている口座番号と、利用者がキーボードから入力した暗証番号とが、金融取引端末４から照合手段６に送られる。照合手段６は金融取引端末４から受け取った口座番号，暗証番号を暗証番号データベース２と照合して確認すると、金融取引端末４に対して取引要求（払い出し金額）の入力を指示し、金融取引端末４からの取引要求と口座番号とを取引実行手段７に渡す。取引実行手段７は元帳データベース３を参照し、取引可能な場合は元帳データベース３を更新して金融取引端末４に取引許可を通知する。これにより金融取引端末４から要求された金額の現金の払い出しが行われて金融取引が終了する。なお、通帳を使用した場合には記帳が行われる。

【００１９】続いて、個人認証情報を登録済みの利用者が通帳もキャッシュカードも携帯していない場合に金融取引を行う場合について説明する。利用者は金融取引端末４で個人認証取引（個人認証情報の確認による取引）を選択し、キーボードから氏名を入力すると共に、指紋採取部にあらかじめ決められている指を押し当てて指紋を入力する。金融取引端末４は、指紋採取部で採取した指紋イメージを解析して指紋特徴を抽出し、抽出した指紋特徴を個人認証情報として入力された氏名と共に個人認証手段５に転送する。個人認証手段５は転送された氏名により個人認証用データベース１を検索し、該当する氏名の個人認証情報と転送された個人認証情報との照合を行う。同姓同名の利用者が多い場合には登録されている複数の個人認証情報との照合を行い一致するものを選択する。照合の結果、一致するものがあれば、一致した個人認証情報に対応する口座番号と暗証番号とを照合手段６に送る。照合手段６は個人認証手段５から転送された口座番号，暗証番号を暗証番号データベース２と照合して確認すると、金融取引端末４に対して取引要求の入力を指示し、前述した通帳またはキャッシュカードを使用した通常の金融取引の場合と同様に取引実行手段７によって金融取引が実行される。この際、同一人が複数の口座を開設している場合には、金融取引端末４の画面に口座種別，口座番号等を表示して一つを選択させるなどの処理を行うようにする。

【００２０】なお、通帳またはキャッシュカードを携帯しているが暗証番号を忘れた場合には、利用者は通帳またはキャッシュカードを金融取引端末４に挿入し、指紋採取部から指紋を入力する。この場合は、個人認証手段５は金融取引端末４から転送される口座番号で個人認証用データベース１を検索し、１回の照合で個人認証情報の確認を行うことができ、同姓同名の利用者が多い場合でも本人確認が短時間で終了する。確認後は転送された口座番号に暗証番号を付加して照合手段６に転送し、前述の場合と同様の処理が行われる。この際、暗証番号を金融取引端末４に転送して利用者に通知する処理を同時に行ってもよい。なお、暗証番号を利用者に通知する処理のみで金融取引は行わないようにすることもできる。

【００２１】上述したように、通帳またはキャッシュカードと暗証番号とを併用する現行の金融取引方式に対して、計算センタに個人認証手段５と氏名を主検索キーとして個人認証情報，口座番号，暗証番号を格納した個人認証用データベース１とを設置し、本店および各支店には指紋採取部を備えた金融取引端末４を少なくとも１台追加して配置することにより、あらかじめ指紋等の個人認証情報を登録した利用者は、暗証番号を忘れた場合や通帳もキャッシュカードも携帯していない場合でも取引が行える新規サービスを提供することが可能となる。なお、個人認証用データベース１に氏名を主検索キーとして個人認証情報を登録することにより、通帳もキャッシュカードも携帯していない場合でも、照合の対象を制限し短時間で認証を行うことが可能となる。

【００２２】以上の説明では、個人認証用データベースには、氏名を主検索キーとして個人認証情報，口座番号，暗証番号が格納されており、あらかじめ登録した利用者は通帳もキャッシュカードも携帯していない場合でも取引できる場合について述べたが、暗証番号を忘れた場合に対するサービスのみを提供する場合には、個人認証用データベースには、口座番号を主検索キーとして個人認証情報，暗証番号を格納しておけばよい。

【００２３】なお、個人認証用データベースを利用することにより、上述した暗証番号を忘れた場合や通帳もキャッシュカードも携帯していない場合に対応するサービス以外にも、本人しか利用できない本人専用口座を設定するなどの新規サービスの提供も可能となる。又、本人確認に使用できる個人認証情報としては指紋が最も一般的であるが、指紋以外にも網膜模様や声紋や自筆署名（筆跡）などを使用することも考えられる。

【００２４】図２は、本発明の第２の実施の形態の構成

を示すブロック図である。本実施の形態は、現金自動入出金業務について相互提携を行っている複数の金融機関が、共同で一つの個人認証用データベースを設置した場合である。Ａ銀行センタ２０及びＢ銀行センタ４０と専用線で接続されているＣＤ提携センタ５０に、接続交換機８を介して個人認証手段５ｃ，個人認証用データベース１ｃが設置されている。Ａ銀行センタ２０，Ｂ銀行センタ４０には、それぞれ図１の第１の実施の形態の計算センタと同様に、暗証番号データベース２ａ，２ｂと、元帳データベース３ａ，３ｂと、照合手段６ａ，６ｂと、取引実行手段７ａ，７ｂとが設置されており、Ａ銀行センタ２０，Ｂ銀行センタ４０とそれぞれ専用線で接続されているＡ銀行本支店１０，Ｂ銀行本支店３０には、金融取引端末４ａ，４ｂが設置されている。

【００２５】金融取引端末４ａ，４ｂから行われる個人認証取引に係わる情報は、自行取引か他行取引かを問わずＡ銀行センタ２０，Ｂ銀行センタ４０を経由してＣＤ提携センタ５０に転送され、接続交換機８を経て個人認証手段５ｃに渡される。個人認証手段５ｃは、渡された氏名（又は口座番号）により個人認証用データベース１ｃを検索して個人認証情報の照合を行い、一致するものがあれば該当する口座番号と暗証番号とを抽出し、口座番号に含まれる銀行識別情報を判断して、該当する銀行の計算センタ（Ａ銀行センタ２０又はＢ銀行センタ４０）に送る。計算センタでは、照合手段６ａ，６ｂが口座番号と暗証番号の正当性を確認すると、要求元の金融取引端末４ａ又は４ｂに対して取引要求の入力を指示し、通常の場合と同様に金融取引が行われる。なお、通帳もキャッシュカードも携帯していない氏名入力の場合には、照合する対象数を少なくし個人認証を短時間で終了させるため、氏名のほかに銀行名等の補助情報をキー入力または選択入力させるようにするとよい。

【００２６】この実施の形態の場合には、複数の銀行に複数の口座を有する利用者は、銀行ごと若しくは口座ごとに異なる暗証番号が設定されていたとしても、すべての口座を登録することにより、口座番号と暗証番号との対応をすべて正確に覚えていなくても必要に応じて希望の口座で取引が可能となり、暗証番号の一元管理ができることになる。

【００２７】図３は、本発明の第３の実施の形態の構成を示すブロック図である。本実施の形態は、本人確認業務を専門に扱う個人認証機関を使用する場合である。Ａ銀行センタ２１，Ｂ銀行センタ４１と専用線で接続されたＣＤ提携センタ５１は、専用線により個人認証手段５ｃ’，個人認証用データベース１ｃ’を備えた個人認証機関６０と接続されている。Ａ銀行本支店１１，Ｂ銀行本支店３１に設置されている金融取引端末４ａ’，４ｂ’からの個人認証取引に係わる情報は、専用線でなくオープンネットワーク７０を介して個人認証機関６０に送られ、個人認証手段５ｃ’が個人認証用データベース１ｃ’を参照して個人認証を行う。本人確認が行われると、口座番号と暗証番号とがＣＤ提携センタ５１を経て該当する銀行の計算センタ（Ａ銀行センタ２１又はＢ銀行センタ４１）に送られ、金融取引が行われる。個人認証機関６０は、オープンネットワーク７０を介して他業種施設８０とも接続されており、個人認証用データベース１ｃ’には、銀行取引に必要な口座番号と暗証番号以外の他業種用の必要情報も格納されているが、要求元の識別情報により、銀行本支店の金融取引端末からの認証要求に対しては、当該銀行の口座番号と暗証番号とを抽出して転送する。

【００２８】

【発明の効果】以上詳細に説明したように、本発明の個人認証を利用した金融取引方式は、通帳またはキャッシュカードと暗証番号とを併用する現行の方式に対して、個人特有の指紋等の個人認証情報を利用した本人確認を併用する構成である。このために、現在の設備を活用しながら、あらかじめ登録した利用者に対して、本人ならば暗証番号を忘れた場合や、通帳もキャッシュカードも携帯していない場合でも取引を可能とする等の新規サービスを提供できる効果がある。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の構成を示すブロック図である。

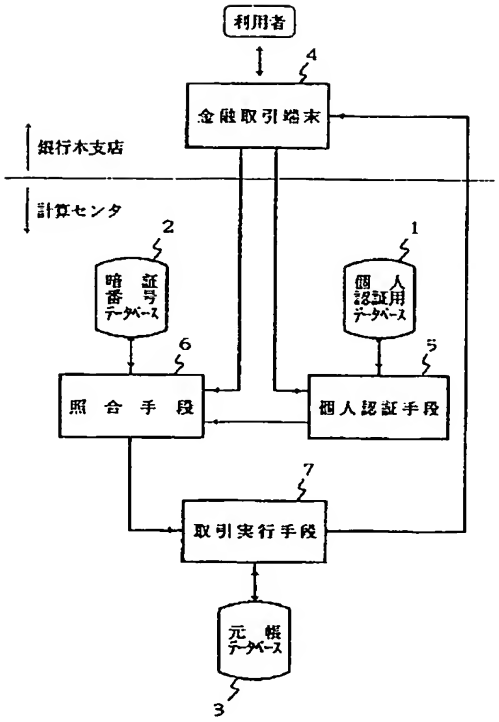
【図２】本発明の第２の実施の形態の構成を示すブロック図である。

【図３】本発明の第３の実施の形態の構成を示すブロック図である。

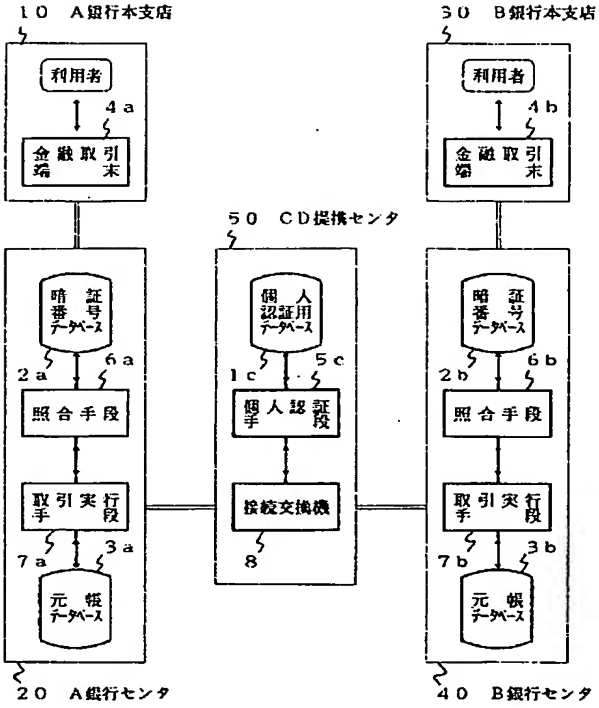
【符号の説明】

１，１ｃ，１ｃ’　個人認証用データベース
２，２ａ，２ｂ　暗証番号データベース
３，３ａ，３ｂ　元帳データベース
４，４ａ，４ａ’，４ｂ，４ｂ’　金融取引端末
５，５ｃ，５ｃ’　個人認証手段
６，６ａ，６ｂ　照合手段
７，７ａ，７ｂ　取引実行手段
８　接続交換機
１０，１１　Ａ銀行本支店
２０，２１　Ａ銀行センタ
３０，３１　Ｂ銀行本支店
４０，４１　Ｂ銀行センタ
５０，５１　ＣＤ提携センタ
６０　個人認証機関
７０　オープンネットワーク
８０　他業種施設

【図１】


利用者
4
金融取引端末
銀行本支店
計算センタ
2
暗証番号データベース
1
個人認証用データベース
6
照合手段
5
個人認証手段
7
取引実行手段
元帳データベース
3

【図２】


10　A銀行本支店
利用者
4a
金融取引端末
暗証番号データベース
2a
6a
照合手段
取引実行手段
7a
3a
元帳データベース
20　A銀行センタ
50　CD提携センタ
個人認証用データベース
1c
5c
個人認証手段
接続交換機
8
30　B銀行本支店
利用者
4b
金融取引端末
暗証番号データベース
2b
6b
照合手段
取引実行手段
7b
3b
元帳データベース
40　B銀行センタ

【図３】

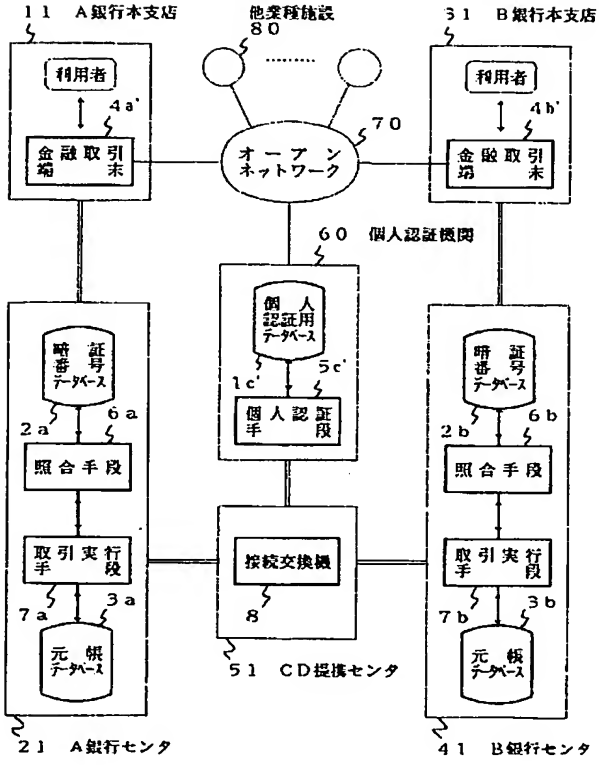

１１　Ａ銀行本支店
他業種施設
８０
３１　Ｂ銀行本支店
利用者
４ａ'
金融取引端末
オープンネットワーク
７０
利用者
４ｂ'
金融取引端末
６０　個人認証機関
個人認証用データベース
１ｃ'
５ｃ'
個人認証手段
暗証番号データベース
２ａ
６ａ
照合手段
取引実行手段
７ａ
３ａ
元帳データベース
２１　Ａ銀行センタ
接続交換機
８
５１　ＣＤ提携センタ
暗証番号データベース
２ｂ
６ｂ
照合手段
取引実行手段
７ｂ
３ｂ
元帳データベース
４１　Ｂ銀行センタ

FIG. 1

【図1】

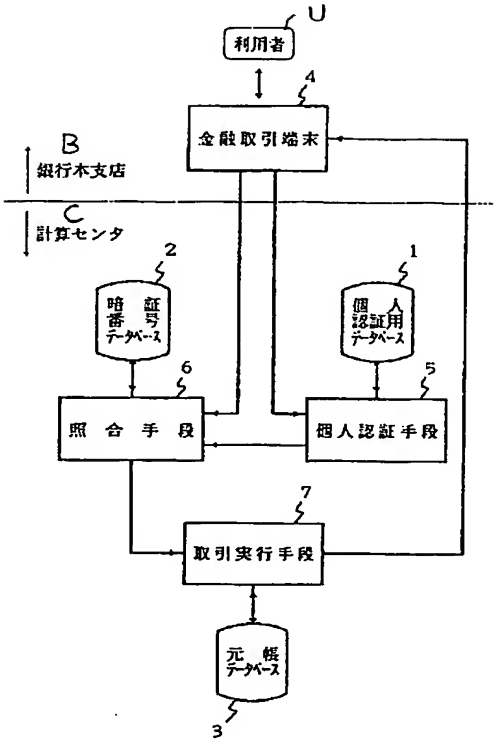
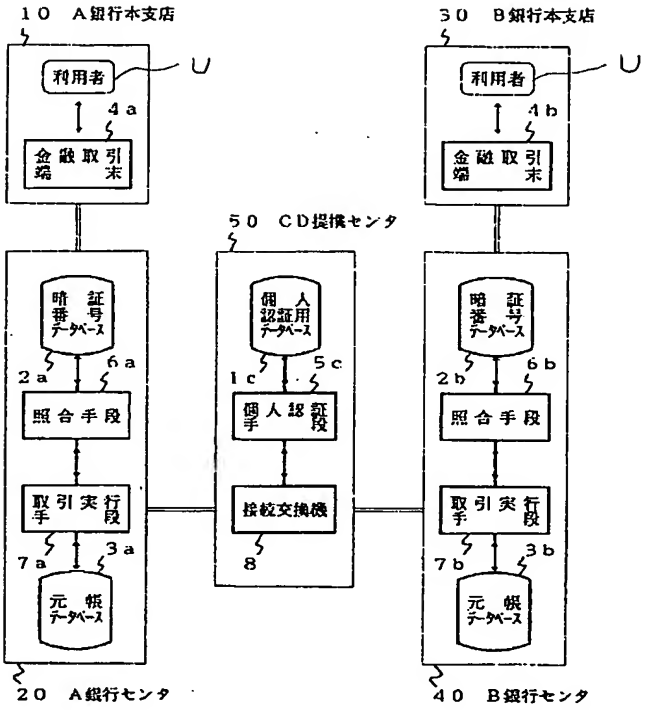


FIG. 2

【図2】

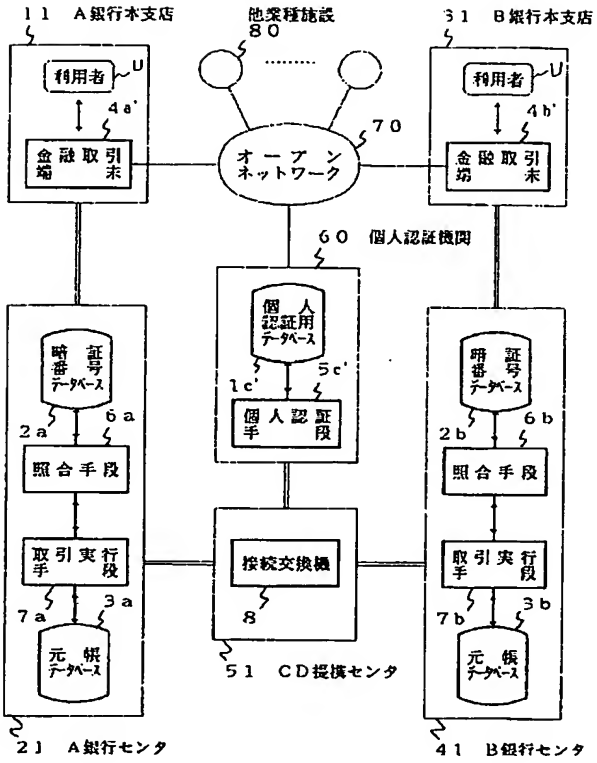


11 --- A BANK HEAD/BRANCH OFFICE
21 --- A BANK CENTER
31 --- B BANK HEAD/BRANCH OFFICE
41 --- B BANK CENTER
51 --- JOINT CD CENTER
60 --- PERSONAL AUTHENTICATION ORGANIZATION
70 --- OPEN NETWORK
80 --- OTHER BUSINESS INSTITUTIONS

U --- USER
1c' --- PERSONAL AUTHENTICATION DATABASE
2a, 2b --- PASSWORD DATABASE
3a, 3b --- LEDEGER DATABASE
4a', 4b' --- FINANCIAL TRANSACTION DATABASE
5, 5c' --- PERSONAL AUTHENTICATION DATABASE
6a, 6b --- MATCHING MEANS
7, 7a, 7b --- TRANSACTION EXECUTING MEANS
8 --- CONNECTING SWITCH

FIG.3

【図3】



1, 1c --- PERSONAL AUTHENTICATION DATABASE

2, 2a, 2b --- PASSWORD DATABASE

3, 3a, 3b --- LEDEGER DATABASE

4, 4a, 4b --- FINANCIAL TRANSACTION DATABASE

5, 5c --- PERSONAL AUTHENTICATION DATABASE

6, 6a, 6b --- MATCHING MEANS

7, 7a, 7b --- TRANSACTION EXECUTING MEANS

8 --- CONNECTING SWITCH

10 --- A BANK HEAD/BRANCH OFFICE

20 --- A BANK CENTER

30 --- B BANK HEAD/BRANCH OFFICE

40 --- B BANK CENTER

50 --- JOINT CD CENTER

U --- USER

B --- BANK HEAD/BRANCH OFFICE

C --- DATA PROCESSING CENTER

11-338947

[SCOPE OF CLAIMS]

[CLAIM 1] A financial transaction system utilizing personal authentication, comprising: a personal authentication database in which personal authentication information used to verify personal identity, account numbers, and passwords are stored with a personal name as a main search key; a password database in which passwords are stored in a one-to-one correspondence with account numbers; a ledger database in which financial transaction information for each account number is stored; a financial transaction terminal equipped with a function to capture personal authentication information and to transfer the same for matching against the personal authentication database; personal authentication means for verifying the personal identify by referring to the personal authentication database based on the personal name or account number and the personal authentication information transferred from the financial transaction terminal, and for outputting both the account number and the password or only the password; matching means for verifying the account number and the password received from the financial transaction terminal or the personal authentication means by matching the same against the password database; and transaction executing means for executing a transaction request received from the financial transaction terminal by referring to the ledger database when the verification is done by the matching means.

[CLAIM 2] A financial transaction system utilizing personal authentication as claimed in claim 1, wherein the personal authentication database and the personal authentication means are provided in common to a plurality of financial institutions, and wherein financial institution identifying information is stored as an auxiliary search key in the personal authentication database.

[CLAIM 3] A financial transaction system utilizing personal authentication as claimed in claim 1, wherein the personal authentication database and the personal

authentication means are provided in a personal authentication organization specializing in personal authentication operations, and wherein the information for matching against the personal authentication database is transferred to the personal authentication organization via an open network, while the account number and the password entered from the financial transaction terminal are transferred to the matching means via a leased line.

[CLAIM 4] A financial transaction system utilizing personal authentication, comprising: a personal authentication database in which personal authentication information used to verify personal identity and passwords are stored with account number as a main search key; a password database in which passwords are stored in a one-to-one correspondence with account numbers; a ledger database in which financial transaction information for each account number is stored; a financial transaction terminal equipped with a function to capture personal authentication information and to transfer the same for matching against the personal authentication database; personal authentication means for verifying the personal identify by referring to the personal authentication database based on the account number and the personal authentication information transferred from the financial transaction terminal, and for outputting the password; matching means for verifying the account number and the password received from the financial transaction terminal or the personal authentication means by matching the same against the password database; and transaction executing means for executing a transaction request received from the financial transaction terminal by referring to the ledger database when the verification is done by the matching means.

[CLAIM 5] A financial transaction system utilizing personal authentication as claimed in claim 4, wherein the account number includes financial institution identifying information, and wherein the personal authentication database and the personal authentication means are provided in common to a plurality of financial institutions.

[CLAIM 6] A financial transaction system utilizing personal authentication as claimed in claim 1, 2, 3, 4, or 5, wherein the personal authentication information is fingerprint information.

[PROBLEM TO BE SOLVED BY THE INVENTION] As described above, the current financial transaction system which uses bankbooks or cash cards in conjunction with passwords affords convenience to customers while ensuring security, but there remains the problem to be solved, in that even a legitimate customer cannot conduct a financial transaction if he forgets his password or if he does not carry a bankbook or a cash card with him.

[0006] One possible approach to solving the above problem would be to use a fingerprint for personal verification, but the method of Japanese Utility Model No. 3043061, described above, that registers fingerprint information in a cash card cannot address the situation unless the customer carries the cash card with him, while the method of Japanese Utility Model Publication No. H01-127051 which uses a fingerprint in conjunction with a password cannot address the situation if the customer forgets his password.

[0007] An object of the present invention is to provide a financial transaction system utilizing personal authentication that can provide improved services to customers; to achieve this, a personal verification scheme utilizing personal authentication information such as a fingerprint unique to each individual person is used in combination with the current system, with provisions made, for example, to allow the legitimate customer to conduct a financial transaction even when he forgets his password or when he does not carry a bankbook or a cash card with him.

[Embodiments of the Invention] Next, embodiments of the present invention will be described with reference to the drawings.

[0015] Figure 1 is a block diagram showing the configuration

of a first embodiment of the present invention. The embodiment shown in Figure 1 concerns the basic configuration of the financial transaction system utilizing personal authentication according to the present invention, which comprises: a personal authentication database 1 in which personal authentication information such as fingerprints is stored; a password database 2 in which passwords are stored in a one-to-one correspondence with account numbers; a ledger database 3 in which financial transaction information for each account number is stored; a financial transaction terminal 4 equipped with a function to capture and transfer personal authentication information such as a fingerprint; a personal authentication means 5 which verifies a person's identify by referring to the personal authentication database 1 based on the person's name or account number and the personal authentication information transferred from the financial transaction terminal 4, and outputs both the account number and the password or only the password; a matching means 6 which verifies the account number and the password received from the financial transaction terminal 4 or the personal authentication means 5 by matching them against the password database 3; and a transaction executing means 7 which, when the verification is done by the matching means 6, executes a transaction request received from the financial transaction terminal 4 by referring to the ledger database 3.

[0016] Of the above constituent elements, the personal authentication database 1, the password database 2, the ledger database 3, the personal authentication means 5, the matching means 6, and the transaction executing means 7 are installed in a data processing center of a financial institution such as a bank, and are connected via a leased line to the financial transaction terminal 4 which is installed in the bank's head office, or in each branch office, for use by customers. The financial transaction terminal 4 is a terminal from which a customer with preregistered personal authentication information such as a

fingerprint can conduct a transaction even when he forgets his password or when he does not carry a bankbook or a cash card with him; the terminal is equipped, in addition to the functions of the conventional automated teller machine, with a fingerprint capturing section for capturing a fingerprint and a feature analyzing section for analyzing the captured fingerprint image and thereby extracting fingerprint features. Though not shown in Figure 1, conventional automated teller machines that enable customers to make transactions using bankbooks, cash cards, and passwords are also installed in the bank's head office and branch offices for use by customers.

[0017] The personal authentication database 1 is a database in which personal authentication information of preregistered customers is stored; the database stores the personal authentication information, account numbers, and passwords with personal name as the main search key, and also allows a search to be conducted using an account number as the search key.

[0018] Operation in Figure 1 will be described below. First, in the case of a usual financial transaction that uses a bankbook, cash card, and password, the account number recorded on the bankbook or cash card that the customer inserted and the password that the customer entered from the keyboard are transmitted from the financial transaction terminal 4 to the matching means 6. The matching means 6 matches the account number and the password received from the financial transaction terminal 4 against the password database 2 and, upon verification, instructs the financial transaction terminal 4 to enter a transaction request (the amount of money to be withdrawn) and passes the account number and the transaction request received from the financial transaction terminal 4 on to the transaction executing means 7. The transaction executing means 7 refers to the ledger database 3 and, if the transaction is possible, then updates the ledger database 3 and sends a transaction permit notification to the financial transaction terminal 4.

Thereupon, the financial transaction terminal 4 dispenses cash in the requested amount, thus completing the financial transaction. When the bankbook is inserted, the transaction is also recorded on the bankbook.

[0019] Next, a description will be given of how the customer with preregistered personal authentication information conducts a financial transaction when he does not carry a bankbook or a cash card with him. The customer selects a personal-authentication-based transaction (a transaction based on the verification of the personal authentication information) on the financial transaction terminal 4, and enters his name from the keyboard as well as his fingerprint by pressing his predesignated finger onto the fingerprint capturing section. The financial transaction terminal 4 extracts fingerprint features by analyzing the fingerprint image captured by the fingerprint capturing section, and transmits the extracted fingerprint features as the personal authentication information to the personal authentication means 5 together with the name that the customer entered. The personal authentication means 5 searches the personal authentication database 1 by using the received name, and checks the received personal authentication information against the personal authentication information that matches the name. If there are a plurality of preregistered customers with the same name, the received personal authentication information is matched against a plurality of pieces of personal authentication information to find a match. If a match is found as a result of the matching, the account number and the password corresponding to the matching personal authentication information are transferred to the matching means 6. The matching means 6 matches the account number and the password transferred from the personal authentication means 5 against the password database 2 and, upon verification, instructs the financial transaction terminal 4 to enter a transaction request, and the financial transaction is then executed by the transaction executing means 7 in the same manner as in the usual financial

transaction performed using the bankbook or the cash card. If the same customer has a plurality of accounts, then the kinds of the accounts, the account numbers, etc. are displayed on the screen of the financial transaction terminal 4 from which the customer makes a selection.

[0020] Here, suppose that the customer forgets his password though he carries a bankbook or a cash card with him; in this case, the customer inserts the bankbook or the cash card into the financial transaction terminal 4, and enters his fingerprint from the fingerprint capturing section. In this case, the personal authentication means 5 searches the personal authentication database 1 by using the account number transferred from the financial transaction terminal 4, and can thus verify the personal authentication information in a single matching operation; even if there are many preregistered customers with the same name, verification of the customer's identity can be finished in a short time. After the verification, the received account number and its associated password are transferred to the matching means 6 where the same processing as earlier described is performed. At the same time, processing may be performed to transfer the password to the financial transaction terminal 4 for notification to the customer. Here, provisions may be made to only notify the customer of the password but not perform any financial transactions.

[0021] As described above, in the current financial transaction system that uses bankbooks or cash cards in combination with passwords, the personal authentication means 5 and the personal authentication database 1, in which personal authentication information, account numbers, and passwords are stored with personal name as the main search key, are additionally installed in the data processing center, and at least one financial transaction terminal 4 equipped with the fingerprint capturing section is additionally installed in each branch office as well as in the head office; this makes it possible to offer a new service that enables any customer with preregistered

fingerprint or other personal authentication information to conduct a financial transaction even when he forgot his password or when he does not carry a bankbook or a cash card with him. Furthermore, by registering the personal authentication information in the personal authentication database 1 with personal name as the main search key, it becomes possible to accomplish the authentication in a short time by limiting the scope of matching even when the customer does not carry a bankbook or a cash card with him.

[0022] The above description has dealt with the case where the personal authentication information, account numbers, and passwords are stored in the personal authentication database with personal name as the main search key, thereby enabling any preregistered customer to conduct a financial transaction even when he does not carry a bankbook or a cash card with him; on the other hand, if the service is to be provided only for the case where the customer forgot his password, the personal authentication information and the passwords should be stored in the personal authentication database with account number as the main search key.

[0023] Further, by using the personal authentication database, a new service such as the service that enables the customer to open his own special account nobody else can use can be provided in addition to the above-described services provided for the case where the customer forgot his password or where he does not carry a bankbook or a cash card with him. Fingerprints are the most commonly used personal authentication information that can be utilized to verify customer identify, but instead of fingerprints, use may be made of other characteristics such as retina patterns, voice prints, or signatures (handwriting).

[0024] Figure 2 is a block diagram showing the configuration of a second embodiment of the present invention. This embodiment concerns the case where a single personal authentication database is installed so as to be shared among a plurality of financial institutions cooperating in automatic cash depositing/dispensing operations. A personal

authentication means 5c and a personal authentication database 1c are installed in a joint CD center 50 which is connected to an A bank center 20 and a B bank center 40 via respective leased lines. The A bank center 20 and the B bank center 40 each include a password database 2a, 2b, a ledger database 3a, 3b, a matching means 6a, 6b, and a transaction executing means 7a, 7b, as in the data processing center of the first embodiment shown in Figure 1, and financial transaction terminals 4a and 4b are installed in the A bank's head office or branch office 10 and the B bank's head office or branch office 30, respectively, which are connected to the A bank center 20 and the B bank center 40 via respective leased lines.

[0025] Information associated with the personal-authentication-based transaction being conducted from the financial transaction terminal 4a or 4b, whether it be an intra-bank transaction or an inter-bank transaction, is transmitted to the joint CD center 50 via the A bank center 20 or the B bank center 40, respectively, and passed to the personal authentication means 5c via a connecting switch 8. Using the customer name (or account number) thus transferred, the personal authentication means 5c searches the personal authentication database 1c for information that matches the personal authentication information; if matching information is found, the personal authentication means 5c extracts the corresponding account number and password, checks bank identifying information included in the account number, and transmits the account number and the password to the data processing center of the corresponding bank (the A bank center 20 or the B bank center 40). At the data processing center, the matching means 6a or 6b verifies the authenticity of the account number and the password, and instructs the requesting financial transaction terminal 4a or 4b to enter a transaction request, and thereafter the financial transaction is performed in the same manner as usual. In the case of a transaction that uses only the customer name and that does not use a bankbook or a password, provisions should be made

to have the customer enter auxiliary information, such as the bank name, in addition to the customer name in order to narrow the scope of matching so that the personal authentication can be accomplished in a short time.

[0026] In this embodiment, even when the customer has different accounts with different banks, and has different passwords set for the different banks or different accounts, if all the accounts are preregistered the customer can conduct a transaction using any desired account even when he does not correctly remember the password for each account, and thus the passwords can be managed centrally.

[0027] Figure 3 is a block diagram showing the configuration of a third embodiment of the present invention. This embodiment concerns the case where verification of customer authenticity is entrusted to a specialized personal authentication organization. A joint CD center 51, which is connected to an A bank center 21 and a B bank center 41 via respective leased lines, is connected via a leased line to a personal authentication organization 60 equipped with a personal authentication means 5c' and a personal authentication database 1c'. Information associated with the personal-authentication-based transaction being conducted from a financial transaction 4a' or 4b' installed in the A bank's head office or branch office 11 or the B bank's head office or branch office 31, respectively, is transmitted via an open network 70, not via a leased line, to the personal authentication organization 60 where the personal authentication means 5c' performs personal authentication by referring to the personal authentication database 1c'. When the customer's identity is verified, the account number and the password are sent via the joint CD center 51 to the data processing center of the corresponding bank (the A bank center 21 or the B bank center 41), and the financial transaction is thus conducted. The personal authentication organization 60 is also connected to other business institutions 80 via the open network 70, and not only account numbers and passwords necessary for bank transactions but

information necessary for other businesses is also stored in the personal authentication database 1c'; here, for an authentication request received from the financial transaction terminal of the bank's head office or branch office, the requesting bank is identified based on its identifying information and the account number and password for that bank are extracted for transmission.

[0028]

[Advantageous Effect of the Invention] As described in detail above, in the financial transaction system utilizing personal authentication according to the present invention, a personal verification scheme utilizing personal authentication information such as a fingerprint unique to each individual person is used in combination with the current system that uses a bankbook or cash card in combination with a password. Therefore, while making use of the existing equipment, the present invention offers the effect of being able to provide a new service such as the service that enables any preregistered customer to conduct a financial transaction even when he forgets his password or when he does not carry a bankbook or a cash card with him, as long as his authenticity can be verified.